APPENDIX I

Functional Specification for the
Trade Secret Examiner
Trade Secret Documentation Tool

Table of Contents

Functional Specification For The
Trade Secret Examiner
Trade Secret Documentation Tool

1 Document Information

1.1 Description

This document is a top-level functional specification for the Trade Secret Examiner Trade Secret Documentation Tool.

1.2 Scope

This document shall describe all necessary functions, features, and interfaces of the Trade Secret Examiner Trade Secret Documentation Tool.

1.3 Authorship

The authors of this document are: R. Mark Halligan and Richard F. Weyand.

1.4 Ownership

1.5 Revision History

Rev	Reviser	Date	Description
0.0	R. F. Weyand	11/25/99	New document.
0.1	R. F. Weyand	12/2/99	Incorporate RMH review comments. Other changes & additions throughout.
0.2	R. F. Weyand	12/19/99	Incorporate RMH review comments. Other changes & additions throughout.
0.3	R. F. Weyand	1/10/00	Patent changes & additions throughout.

2 Overview

2.1 Purpose

The Trade Secret Examiner Trade Secret Documentation Tool is intended as an automated aid for the documentation, analysis, auditing, accounting, protection, and other management of the trade secret intellectual property of individuals and corporations. Its overall purpose is to provide automated assistance in the

performance of these tasks, lowering administrative costs and increasing the security and defendability of trade secret intellectual property.

2.2 Goals

The goals of the Trade Secret Examiner Trade Secret Documentation Tool are:

- To automate the entry of trade secret information.
- To automate the indexing and cataloguing of trade secrets.
- To automate the prioritization of trade secrets.
- To automate analysis and reporting about trade secrets.
- To facilitate the valuation and accounting of trade secrets.
- To facilitate the implementation and analysis of proper security for trade secrets.
- To automate the management of employee issues relating to trade secrets.
- To provide registration and verification of the existence, ownership, contents, and other information relating to trade secrets.
- To prepare reports and court exhibits documenting employee and outsider exposure to trade secrets prior to and during litigation.

2.3 Feature Packages

Trade Secret Examiner shall be structured into feature packages, or revisions, that stage the introduction of the described features over several releases. The releases and their goals shall be as follows:

- **Release 1.0** -- Commercially viable corporate server and small server products that include database features required to support the full feature set of this specification, and include trade secret data entry and basic analysis tools.
- **Release 2.0** – Enhanced server products that include more advanced analysis tools.
- **Release 3.0** – Addition of single-user product; further enhancement of analysis tools.
- **Release 4.0** – SAP and PeopleSoft interfaces for employee data; further enhancement of analysis tools to provide employee management features.
- **Release 5.0** – Low-cost PC data-entry version.

Details of the features to be contained in each feature package are documented in Appendix A.

2.4 Glossary

Company data – data entered into Trade Secret Examiner that documents policies and characteristics of the company.

Configuration data – data entered into Trade Secret Examiner that configures the operation of Trade Secret Examiner to meet company needs.

Drilling down – the process of investigating one item in a list by selecting it, and thereby opening a window showing the underlying data for this entry.

Employee data – data entered into Trade Secret Examiner that is specific to individual employees.

Fuzzy search – a search method whereby exact matches are not necessary.

Regular expressions – a UNIX operating system term for writing search criteria.

Six factors – six properties of a trade secret recognized by the courts as determining the existence and value of a trade secret.

Trade secret management data – data entered into Trade Secret Examiner for the management of trade secret data.

Trade secret application data – data entered into Trade Secret Examiner for the documentation of a trade secret.

Trade secret derived data – data derived by Trade Secret Examiner from other data about a trade secret.

Trade secret data – data entered into Trade Secret Examiner that is specific to a trade secret.

3 Architecture

Trade Secret Examiner shall be available on four architectures:

- Corporate server architecture.
- Small server architecture.
- Single-user architecture.
- Personal computer architecture.

The database created by Trade Secret Examiner shall be portable across all four architectures in both directions, although not all features and methods of data manipulation shall be supported in all four architectures.

3.1 Corporate Server Architecture

3.1.1 Target Customer

The corporate server architecture shall be aimed at Fortune 1000 companies and high-technology companies. It shall be available at multiple licensing levels to support differently sized databases and different numbers of seats.

3.1.2 Stability And S curity

As the contents of the database of Trade Secret Examiner will generally itself constitute one of the largest trade secrets of the company, the corporate server architecture shall have the stability and security required to secure this asset. In particular, multiple computers, firewalls, and other such devices may be used to implement the corporate server architecture.

3.1.3 Third-Party Suppliers

The corporate server architecture shall be constructed using hardware and software components from third-party suppliers where possible. In particular, computer hardware, operating systems, relational databases, and networking software shall be obtained from third-party suppliers. Preference shall be given to third-party suppliers on the basis of their reputations and their status as de facto standards more than cost.

3.1.4 Platform

The hardware and software platform of the corporate server architecture shall be sufficiently powerful to support a database containing one million trade secrets and five hundred thousand employees, and all the associated data and records.

The hardware and software platform of the corporate server architecture shall be sufficiently powerful to support an administrative user group of 100 simultaneous logons.

3.1.5 Backup Device

The corporate server architecture shall contain a backup device capable of backing up the entire trade secret database.

3.1.6 System Interfaces

The corporate server architecture shall contain the following system interfaces:

- An interface to the Trade Secret Office's Trade Secret Directory server.
- An interface to SAP for obtaining employee data.
- An interface to PeopleSoft for obtaining employee data.

3.2 Small Server Architecture

3.2.1 Target Customer

The small server architecture shall be aimed at medium-sized companies, lower technology companies, and intellectual property law firms. It shall be available at multiple licensing levels to support differently sized databases and different numbers of seats.

3.2.2 Stability And S curity

As the contents of the database of Trade Secret Examiner will generally itself constitute one of the largest trade secrets of the company, the small server architecture shall have the stability and security required to secure this asset.

3.2.3 Third-Party Suppliers

The small server architecture shall be constructed using hardware and software components from third-party suppliers where possible. In particular, computer hardware, operating systems, relational databases, and networking software shall be obtained from third-party suppliers. Preference shall be given to third-party suppliers on the basis of their reputations and their status as de facto standards more than cost.

3.2.4 Platform

The hardware and software platform of the corporate server architecture shall be sufficiently powerful to support a database containing one hundred thousand trade secrets and fifty thousand employees, and all the associated data and records.

The hardware and software platform of the corporate server architecture shall be sufficiently powerful to support an administrative user group of 20 simultaneous logons.

3.2.5 Backup Device

The corporate server architecture shall contain a backup device capable of backing up the entire trade secret database.

3.2.6 System Interfaces

The corporate server architecture shall contain the following system interfaces:

- An interface to the Trade Secret Office's Trade Secret Directory server.
- An interface to SAP for obtaining employee data.
- An interface to PeopleSoft for obtaining employee data.

3.3 Single-User Architecture

3.3.1 Target Customer

The single-user architecture shall be aimed at small companies and intellectual property lawyers.

3.3.2 Stability And Security

The single-user architecture shall have the stability and security required to provide a robust platform for the Trade Secret Examiner, but need not provide all of the security of the server architectures.

3.3.3 Third-Party Suppli rs

The single-user architecture shall be constructed using hardware and software components from third-party suppliers where possible. In particular, computer hardware, operating systems, relational databases, and networking software shall be obtained from third-party suppliers. Preference shall be given to third-party suppliers on the basis of their reputations and their status as de facto standards more than cost.

3.3.4 Platform

The hardware and software platform of the corporate server architecture shall be sufficiently powerful to support a database containing twenty thousand trade secrets and ten thousand employees, and all the associated data and records.

3.3.5 Backup Device

The corporate server architecture shall contain a backup device capable of backing up the entire trade secret database.

3.3.6 System Interfaces

The corporate server architecture shall contain the following system interfaces:

- An interface to the Trade Secret Office's Trade Secret Directory server.
- An interface to SAP for obtaining employee data.
- An interface to PeopleSoft for obtaining employee data.

3.4 Personal Compute r Architecture

The personal computer architecture shall be aimed at consultants, inventors, and intellectual property lawyers.

3.4.1 Stability And Security

The personal computer architecture shall not provide security features beyond those typically available on personal computer platforms.

3.4.2 Third-Party Suppliers

The personal computer architecture shall be constructed using IBM PC clones, Microsoft Windows operating systems, and other components from third-party suppliers where possible. In particular, relational databases and networking software shall be obtained from third-party suppliers. Preference shall be given to third-party suppliers on the basis of their reputations and their status as de facto standards more than cost.

3.4.3 Platform

The hardware and software platform of the corporate server architecture shall be sufficiently powerful to support a database containing twenty thousand trade secrets and ten thousand employees, and all the associated data and records.

3.4.4 Backup Device

The corporate server architecture shall contain a backup device capable of backing up the entire trade secret database.

3.4.5 System Interfaces

The corporate server architecture shall contain the following system interfaces:

- An interface to the Trade Secret Office's Trade Secret Directory server.

4 Access

Three different kinds of access shall be provided:

- Data entry by employees or contractors involved in the documentation of the trade secret, including outside or inside counsel performing trade secret audits. This access will take the form of filling out a Trade Secret Application. This access is write-once access only. This access shall be designed to meet the rules for client-attorney communications.
- Administrative access by attorneys and their assistants involved in the management of the trade secret, including analysis and reporting preparatory and during trade secret litigation. This access is read-write access. This access shall be designed to meet the rules for attorney work product. This access method shall be password protected. Password timeouts shall be a configurable option, with configurable timeout periods.
- Superuser access by attorneys and their assistants involved in the system administration of Trade Secret Examiner itself. This access is read-write access. This access shall be designed to meet the rules for attorney work product. This access method shall be password protected. Password timeouts shall be a configurable option, with configurable timeout periods.

4.1 Data Entry By Employees and Contractors

At least three methods of data entry shall be provided for the entry of trade secret application data by employees and contractors involved in the creation and documentation of trade secrets.

- Word entry
- Email entry
- Web page entry

4.1.1 Word Entry

Word entry shall consist of data entry via a document file created with the Microsoft Word word processing application. Employees and contractors of the firm shall be able to enter all trade secret application data using a Microsoft Word document template requested from the system or provided on floppy disk or other media. The template shall include all necessary data fields and provide options for values for necessary selections. A method shall be provided to include on the floppy disk or other media any related files required to document the trade secret.

Entry made via this method shall be performed within a Microsoft Word document input routine provided within the administrative access user interface.

This entry method shall be provided on all system architectures.

4.1.2 Email Entry

Email entry shall consist of data entry via an email to the Trade Secret Examiner system over the company intranet. Employees and contractors of the firm shall be able to enter all trade secret application data using an email template requested from the system. The template shall include all necessary data fields and provide options for values for necessary selections. A method shall be provided to upload any related files required to document the trade secret.

Entry made via this method shall be checked to ensure it originates within the company. Entry deemed not originating within the company shall be queued for immediate review and acceptance or rejection by attorneys or their assistants.

This entry method shall be provided on all system architectures.

4.1.3 Web Page Entry

Web page entry shall consist of data entry via a web page on the company intranet. Employees and contractors of the firm shall be able to enter all trade secret application data using a web page form that includes the necessary data fields and check marks for the necessary selections. A method shall be provided to upload any related files required to document the trade secret.

Entry made via this method shall be checked to ensure it originates within the company. Non-repudiation or other methods may be used. Entry deemed not originating within the company shall be queued for immediate review and acceptance or rejection by attorneys or their assistants.

This entry method shall be provided on the secure server architecture.

4.2 Administrative Access By Attorneys And Their Assistants

Four methods of access shall be provided for access to trade secret application data, trade secret management data, trade secret derived data, and some other data by attorneys and their assistants involved in the management of trade secrets.

- Administrative access via the server console.
- Administrative access via directly connected LAN.
- Administrative access via known IP address.
- Administrative access via known-number dial-back login.

4.2.1 Access Via The Server Console

Access via the server console shall be a full user interface that shall be available on the console of the application server.

This access shall be able to be optionally disabled.

This access method shall be provided on all system architectures.

4.2.2 Access Via Directly Connected LAN

Access via directly connected LAN shall be a full user interface that shall only work from client machines on the same IP network address as the application server. Check of the IP address, check of the MAC-level address, check of the IP time-to-live field, non-repudiation, or other methods shall be used to prevent IP address spoofing and other cheats. Periodic discovery of the directly connected LAN shall be performed to generate a list of accessible MAC-level addresses.

This access shall be able to be optionally disabled.

This access method shall be provided on the server architectures.

4.2.3 Access Via Known IP Address

Access via known IP address shall be a full user interface that shall only work from client machines with one of the specific IP network addresses specified. Check of the IP address, periodic cross-check of the MAC-level address, check of the IP time-to-live field, non-repudiation, or other methods shall be used to prevent IP address spoofing and other cheats. Addresses on the list of known IP addresses shall have one of two expiration time-outs associated with them: expiration on an explicit date; expiration after a specified time period. The maximum time-to-expire for known IP addresses in the system shall be a configurable option.

This access shall be able to be optionally disabled.

This access method shall be provided on the secure server architectures.

4.2.4 Access Via Known-Number Dial-Back Login

Access via known-number dial-back login shall be a full user interface that shall only work from client machines that has been called from the application server. This call shall be initiated by a dial-in attempt from a known telephone number, as read from the ANI signal of the dial-in line. Telephone numbers on the list of known numbers shall have one of two expiration time-outs associated with them: expiration on an explicit date; expiration after a specified time period. The

maximum time-to-expire for known telephone numbers in the system shall be a configurable option.

This access shall be able to be optionally disabled.

This access method shall be provided on the secure server architectures.

4.3 Superuser Access

Superuser access shall be from the console of the application server only. This access shall provide the following functions, which shall not be available from any other interface or access method:

- Changing the list of network IDs defined to be within the company.
- Enabling or disabling administrative access via the server console.
- Enabling or disabling administrative access via directly connected LAN.
- Enabling or disabling administrative access via known IP address.
- Changing the list of known IP addresses.
- Changing the expiration dates of known IP addresses.
- Enabling or disabling administrative access via known-number dial-back login.
- Changing the list of known telephone numbers.
- Changing the expiration dates of known telephone numbers.
- Creating user names for administrative access.
- Resetting passwords for administrative access.
- Mounting other applications on the application server.
- Backing up the trade secret database.
- Restoring the trade secret database from backup.

5 Trade Secret Data

The basic record of Trade Secret Examiner is the trade secret record. Trade secret data within a trade secret record is divided into three types:

- Trade secret application data. This data is entered by the employees and contractors involved in the documentation of the trade secrets.
- Trade secret management data. This data is entered by the attorneys and their assistants involved in the management of the trade secrets.
- Trade secret derived data. This data is derived by Trade Secret Examiner from other data about the trade secrets.

Many of the trade secret data fields of the trade secret record can be configured to be either application data, management data, or derived data. Each of the trade secret data fields specifies which types of trade secret data the field can be configured to be.

5.1 Trade Secret Application Data

Trade secret application data shall be able to be entered from within the **Data Entry By Employees and Contractors** access method or from within the **Administrative Access By Attorneys And Their Assistants** access method. Trade secret application data can only be viewed from within the **Administrative Access By Attorneys And Their Assistants** access method.

5.2 Trade Secret Management Data

Trade secret management data shall be able to be entered and viewed only from within the **Administrative Access By Attorneys And Their Assistants** access method.

5.3 Trade Secret Derived Data

Trade secret derived data shall be able to be viewed only from within the **Administrative Access By Attorneys And Their Assistants** access method. This data shall be calculated by the system according to configurable mathematical and logical formulas.

5.4 Trade Secret Data Fields

The following types of trade secret data shall be supported by the system:

5.4.1 Draft Application Number: D

A unique sequential draft application number shall be assigned to each trade secret draft application entered into the system. The first index number shall be 1. Draft application numbers shall not be able to be changed, edited or modified, or reassigned to any trade secret other than the one initially entered under that number.

It shall be possible to configure a three-character alphabetic field to be prepended to the draft application number, such as "ABC".

5.4.2 Application Number: D

A unique sequential application number shall be assigned to each trade secret application entered into the system. The first index number shall be 1. Application numbers shall not be able to be changed, edited or modified, or reassigned to any trade secret other than the one initially entered under that number.

It shall be possible to configure a three-character alphabetic field to be prepended to the application number, such as "ABC".

5.4.3 Application Ha h Codes: D

Hash codes shall be calculated and stored for each trade secret application submitted to the Trade Secret Office's Trade Secret Directory server. The hash codes shall be calculated using deterministic secure one-way hash codes. The size of the hash codes and the calculation method shall be selected for the characteristics of uniformity of distribution and limited probability of duplication.

Several hash codes shall be calculated for each trade secret per the Database Segmentation of Section 12.

It shall always be possible to generate the same hash code at a later date, whether or not the data has been updated in the intervening period.

5.4.4 Certificate Number: D

A unique sequential certificate number shall be recorded for each trade secret certificate granted by the Trade Secret Office's Trade Secret Directory server. Certificate numbers shall not be able to be changed, edited or modified, or reassigned to any trade secret other than the one initially entered under that number.

5.4.5 Certificate Hash Code: D

The hash code received from the Trade Secret Office's Trade Secret Directory server shall be stored for each trade secret in the system.

5.4.6 Name Of The Trade Secret: A

A name for the trade secret shall be a required field. It shall be a configurable option of the system whether or not this name must be unique within the system.

5.4.7 Date The Trade Secret Was Created: A

The date that the trade secret was created shall be a required field. It shall be possible to configure this field to accept text values, such as "Unknown". It shall be possible to specify a date as "On", "About", "After", or "Prior To".

5.4.8 Date The Trade Secret Application Was Entered: D

The date that the trade secret application was entered shall be recorded by the system.

5.4.9 Trade Secret Applicant: A

The name of the person entering the trade secret application shall be a required field. Additional required fields may include the applicant's email address, work location, title/status (employee, contractor, etc.), and other data.

5.4.10 Originating Organization For The Trade Secret: A

A value for the originating organization for the trade secret shall be a required field. This field shall consist of up to five sub-fields. The number of sub-fields

from 1 to 5 shall be a configurable option. The names of the five sub-fields shall be a configurable option. The default number of sub-fields shall be three. The default values for the names of the three default sub-fields shall be:

- Group
- Department
- Division

It shall be a configurable option whether the value of the five sub-fields must match one entry of a list of corporate organizations. The value "All" shall be an acceptable value for any sub-field, providing that all sub-fields below this sub-field within the field are also "All".

5.4.11 Location Where The Trade Secret Was Created: A

The location (which company location, plant, building, or other identifier) where the trade secret was created shall be a required field. It shall be a configurable option whether the location must be selected from a list of company locations. If so configured, another configurable option shall be whether or not "Other" is an acceptable location. If "Other" is an acceptable location, and is selected, a text field defining the other location shall be a required field.

5.4.12 Locations Where The Trade Secret Is Stored: A

The locations (which company location, plant, building, or other identifier) where the trade secret is stored shall be a required field. The entry of multiple locations shall be supported for this field. It shall be a configurable option whether the locations must be selected from a list of company locations. If so configured, another configurable option shall be whether or not "Other" is an acceptable location. If "Other" is an acceptable location, and is selected, a text field defining the other location shall be a required field.

5.4.13 Locations Where The Trade Secret Is Used: A

The locations (which company location, plant, building, or other identifier) where the trade secret is used shall be a required field. The entry of multiple locations shall be supported for this field. It shall be a configurable option whether the locations must be selected from a list of company locations. If so configured, another configurable option shall be whether or not "Other" is an acceptable location. If "Other" is an acceptable location, and is selected, a text field defining the other location shall be a required field.

5.4.14 Keywords Associated With The Trade Secret: A

Several keywords associated with the trade secret to allow indexing and search shall constitute a required field. It shall be a configurable option whether the keyword list must be unique. It shall be a configurable option whether the keyword field has a minimum number of keywords. If so configured, the minimum number of keywords shall be configurable.

5.4.15 Description Of Th Trade Secret: A

A text description of the trade secret shall be a required field.

5.4.16 The Six Factors Of A Trade Secret

An estimated value for the six factors of a trade secret shall be a required field for each trade secret record. The value of the first five shall be from 1 to 5, and each value shall have a configurable text meaning. The sixth factor, security measures, shall be characterized by the actual security measures taken.

The default selections and their meanings for the first five shall be:

5.4.16.1 Inside Knowledge Factor: AM

To whom is the trade secret known within the company?

Whole Company. Generally known within the company.

Within Division. Generally known within the originating division.

Within Department. Generally known within the originating department.

Within Group. Generally known within the originating group.

Select Persons. Known to select persons only.

5.4.16.2 Outside Knowledge Factor: AM

To whom is the trade secret known within the industry?

Generally Known. Generally known within the industry.

Several Segments. Known to companies within several segments of the industry.

Few Companies. Known to only a few specialized companies within the industry.

Few Experts. Known to only a few experts within the industry.

Not Known. Not known within the industry at all.

5.4.16.3 Investment Factor: AM

How much has the company invested in developing this trade secret?

Little Investment. Created by accident in the course of business without much specific investment.

Some Investment. Created as a minor part of a small project with a minor investment.

Considerable Investment. Created as a major part of a small project with a minor investment.

Substantial Investment. Created as a minor part of a large project with a major investment.

Major Investm nt. Created as a major part of a large project with a major investment.

5.4.16.4 Economic Benefit Factor: AM

What is the importance of the economic benefit provided to the company or potentially to its competitors by the trade secret?

Little Importance. Little or no current economic benefit.

Some Importance. Some economic benefit for a portion of the company's activities.

Important. Major economic benefit for a portion of the company's activities.

Very Important. Major economic benefit for many or most of the company's activities.

Extremely Important. Major economic benefit affecting the viability of the company.

5.4.16.5 Reproducibility Factor: AM

How hard would it be for an outside firm to independently reproduce the trade secret?

Easy. Minor effort using off-the-shelf tools and technology or generally available information; within the capabilities of all competitors.

Difficult. Considerable effort, requiring some financial effort, industry expertise, and some time; within the capabilities of most competitors.

Very Difficult. Substantial effort, requiring considerable financial effort, specialized expertise, and considerable time to develop; beyond the capabilities of most competitors.

Extremely Difficult. Major effort, requiring very large financial investments, rare expertise, and substantial time to develop; beyond the capabilities of all but a few competitors.

Impossible. Impossible to reproduce at any cost by any outside firm.

5.4.16.6 Security Measures Factor: AMD

What kind of security precautions has the company taken to protect the trade secret?

The value for this factor shall be configurable to be Application Data, Management Data, or Derived Data. If configured to be Application Data or Management Data, this value shall be entered directly. The default values and their meanings shall be:

Littl Security. Little or no security precautions.

Som S curity. Some precautions, including locked facility and use of passwords.

Much Security. Many security precautions, including locked and alarmed facility, password protection, network firewalls.

Major Security. Major security precautions, including need-to-know distribution, entry cards, off-hours guards, password protection with password timeouts, and limited or no network access.

Intense Security. Intense security precautions, including severely limited distribution, secure computers or equipment, guarded archival facilities or locked vaults.

If configured to be Derived Data, this value shall be derived from a selection of items from a list of security measures. The selection of items shall itself be configurable to be Application Data or Management Data. The list of security measures and their weights in calculating the derived value for this factor shall be configurable. The derived value shall be configurable as a mathematical function of the weightings of the selection items using common mathematical expressions.

The default selection values shall depend on the values entered for **Location Where The Trade Secret Was Created, Locations Where The Trade Secret Is Stored,** and **Locations Where The Trade Secret Is Used**. A different default set of security measures shall be a configurable value for each location in the location list. The value of "None" shall be removed on the selection of any security measure, and reinstated on the removal of all security measures. Selection of "None" shall remove all other security measures.

- None.
- Building doors locked during off-hours.
- Security guard in the building during off-hours.
- Security guard who makes rounds within the building during off-hours.
- Receptionist/guard at each unlocked entrance during office hours.
- Badges required of all persons in the building.
- Badge reader device on all doors of the building.
- Badge reader device access record of all persons entering and leaving the facility.
- Trade secret marked "Confidential".
- Trade secret kept in individually locked room.
- Trade secret kept in locked cabinet.
- Trade secret kept in vault.
- Trade secret kept off-premises in bank vault.

- Trade secret distributed on a need-to-know basis only.
- The employee handbook contains a section describing the employee's responsibilities regarding trade secrets.
- Employees must sign an acknowledgement of reading the employee handbook, which contains a section describing the employee's responsibilities regarding trade secrets.
- Employees must sign employee confidentiality agreement on employment.
- Employees must sign employee confidentiality agreement annually.
- Employees must sign a separate employee confidentiality agreement for disclosure of this trade secret.

5.4.17 Security Threat Factor Of The Trade Secret: AMD

The security threat factor of a trade secret shall be a required field. The value for this field shall be configurable to be Application Data, Management Data, or Derived Data. If configured to be Application Data or Management Data, this value shall be entered directly. The default values and their meanings shall be:

Little Threat. Little or no threat of theft.

Some Threat. Some threat of theft, including occasional visitors and some trade show attendance.

Large Threat. Large threat of theft, including many visitors, frequent trade show attendance, and published papers.

Major Threat. Major threat of theft, including visitors, trade shows, papers, and some employee turnover to competitors.

Intense Threat. Intense threat of theft, including visitors, trade shows, papers, high employee turnover to competitors, and concerted efforts to penetrate the company by competitors.

If configured to be Derived Data, the actual value for the security threat factor shall be derived from a selection of items from a list of threats. The selection of items shall itself be configurable to be Application Data or Management Data. The list of threats and their weights in calculating the derived value for this factor shall be configurable. The derived value shall be configurable as a mathematical function of the weightings of the selection items using common mathematical expressions.

The default values shall depend on the values entered for **Location Where The Trade Secret Was Created, Locations Where The Trade Secret Is Stored,** and **Locations Where The Trade Secret Is Used**. A different default set of threats shall be a configurable value for each location in the location list. The value of "None" shall be removed on the selection of any threat, and reinstated on the removal of all threats. Selection of "None" shall remove all other threats.

- None.

- Trade secret is threatened by third-party visitors to the facility.
- Trade secret is threatened by employee participation in trade shows.
- Trade secret is threatened by employee publication of articles and papers.
- Trade secret is threatened by disclosure by former employees.
- Trade secret is threatened by outside attempts to penetrate the company.

5.4.18 Patentability Of The Trade Secret: AM

A field documenting whether the trade secret is patentable shall be a required field. There is no default value for this field. The possible values for this field shall be:

- Yes.
- No.
- Do not know.

5.4.19 Estimated Life Expectancy Of The Trade Secret: AM

A field documenting the estimated life expectancy of the trade secret shall be a required field. Five estimated life expectancies shall be supported. The first four shall be configurable values, while the fifth value shall be "Perpetual". There is no default value for this field. The default values for this field shall be:

- 1 year.
- 3 years.
- 5 years.
- 10 years.
- Perpetual.

5.4.20 Additional Files Required To Document The Trade Secret: AM

A field naming additional files required to document the trade secret shall be an optional field. These files may be design files, graphics files, text files, or any other computer file. Trade Secret Examiner shall be able to upload and archive these files, and to reference them from within the tool.

5.4.21 Validity Status Of The Trade Secret: M

The validity status of the trade secret shall be a required field containing one of a set of configurable values. The default values shall be:

- **New**. This trade secret has been recently entered and has not undergone legal review.
- **Pending Data**. This trade secret has undergone legal review and requires the entry of further data to be complete.

- **P nding Review**. This trade secret has undergone legal review and requires the business review to be complete.
- **Granted**. This trade secret has undergone both legal and business review, been determined to be a valid trade secret, and the data entry is complete. It has been granted a certificate number by the system
- **Duplicate**. This trade secret has been removed from current status as it has been determined to be a duplicate of another trade secret in the system. If the validity status is "Duplicate", then a "Same As" field containing the index number of the duplicate trade secret shall be a required field.
- **Declassified**. This trade secret has been removed from current status due to becoming independently widely known in the industry.
- **Obsolete**. This trade secret has been removed from current status due to being no longer valuable or relevant to the company's business.
- **Invalid**. This trade secret has undergone both legal and business review, been determined not to be a valid trade secret, and the data entry is complete.

5.4.22 Source Status Of The Trade Secret: M

The source status of the trade secret shall be a required field containing one of a set of configurable values. The default values shall be:

- **In-House**. The company developed this trade secret in-house.
- **Shop Right**. The company has a shop right to the use of this trade secret.
- **Licensed**. The company has licensed the use of this trade secret from a third-party.
- **Purchased**. The company has purchased the use of this trade secret from a third-party.

If the source status of the trade secret is "Shop Rights", "Licensed", or "Sold", additional required fields shall record the "Owner", "Licensed From" or "Purchased From" parties and the terms of the purchase or license.

It shall be an optional field to specify additional files required to document the source status, such as digitally-signed contracts, scanned contract images, or invoice files or images.

5.4.23 Licensing Status Of The Trade Secret: M

The licensing status of the trade secret shall be a required field containing one of a set of configurable values. The default values shall be:

- **Exclusiv** . The company has retained exclusive rights to this trade secret.
- **Licensed**. The company has licensed the use of this trade secret to a third-party.

- **Sold**. The company has sold the use of this trade secret to a third-party.

If the licensing status of the trade secret is "Licensed" or "Sold", additional required fields shall record the "Licensed To" or "Sold To" parties and the terms of the sale or license.

It shall be an optional field to specify additional files required to document the licensing status, such as digitally-signed contracts, scanned contract images, or invoice files or images.

5.4.24 Legal Reviewer Level Of The Trade Secret: M

The legal reviewer level of the trade secret shall be a required field containing one of a set of configurable values. The default values shall be:

- **CLO**. This trade secret must be reviewed by the Chief Legal Officer of the firm.
- **Senior Attorney**. This trade secret must be reviewed by a senior attorney.
- **Associate Attorney**. This trade secret must be reviewed by an associate attorney.
- **Junior Associate**. This trade secret must be reviewed by a junior associate attorney.

5.4.25 Last Legal Review Date: M

The date of last legal review of this trade secret shall be a required field. One acceptable value shall be "Not reviewed" for records with a status of "New" only.

5.4.26 Last Legal Reviewer: M

The reviewer of the last legal review of this trade secret shall be a required field. One acceptable value shall be "Not reviewed" for records with a status of "New" only.

5.4.27 Legal Reviewer Comments: M

The legal reviewer shall be able to enter text comments as an optional field.

5.4.28 Legal Review Schedule: M

The legal review schedule of the trade secret shall be a required field containing one of a set of configurable values. The default values shall be:

- Not required. This value is acceptable for records with a status of "Declassified", "Obsolete", or "Invalid" only.
- Two years.
- One year.
- Six months.
- Three months.

5.4.29 Business Revi w r L v l Of Th Trade S cr t: M

The Business reviewer level of the trade secret shall be a required field containing one of a set of configurable values. The default values shall be:

- **CEO**. This trade secret must be reviewed by the Chief Executive Officer of the firm.
- **CIO**. This trade secret must be reviewed by the Chief Information Officer of the firm.
- **CTO**. This trade secret must be reviewed by the Chief Technical Officer of the firm.
- **Division**. This trade secret must be reviewed by the General Manager of the division.
- **Department**. This trade secret must be reviewed by the department head.

5.4.30 Last Business Review Date: M

The date of last Business review of this trade secret shall be a required field. One acceptable value shall be "Not reviewed" for records with a status of "New", "Pending Data", or "Pending Review" only.

5.4.31 Last Business Reviewer: M

The reviewer of the last Business review of this trade secret shall be a required field. One acceptable value shall be "Not reviewed" for records with a status of "New", "Pending Data", or "Pending Review" only.

5.4.32 Business Reviewer Comments: M

The business reviewer shall be able to enter text comments as an optional field.

5.4.33 Business Review Schedule: M

The Business review schedule of the trade secret shall be a required field containing one of a set of configurable values. The default values shall be:

- Not required. This value is acceptable for records with a status of "Declassified", "Obsolete", or "Invalid" only.
- Two years.
- One year.
- Six months.
- Three months.

5.4.34 Trade Secret Value: AM

The value of a trade secret shall contain the estimated dollar value of the trade secret on a specified date. It shall be a configurable option as to whether this

field is optional or required. If a dollar value is specified, then the date shall be required.

5.4.35 Trad S cret D pr ciation Method and Sch dul : AM

The depreciation method and schedule fields for the trade secret shall be optional fields. Depreciation methods and schedules available shall include all current IRS approved depreciation methods and schedules. It shall also be possible to specify trade secret appreciation with time using similar methods.

5.4.36 Net Present Value: D

The system shall be able to generate the net present value of a trade secret for any date of its existence. The net present value shall be a function of the **Trade Secret Value** fields and the **Trade Secret Depreciation Schedule And Method** fields for each trade secret. This function shall conform to IRS rules and Generally Accepted Accounting Principles for determining the net present value of an asset.

5.4.37 Trade Secret Type: M

The trade secret type shall contain a number corresponding to the general type of trade secret. A list of the general types of trade secret is contained in Appendix B. It shall be a configurable option as to whether this field is optional or required.

5.4.38 Confidentiality Level: AMD

The confidentiality level of a trade secret shall be an optional field. The value for this field shall be configurable to be Application Data, Management Data, or Derived Data. If configured to be Application Data or Management Data, this value shall be entered directly. If configured to be Derived Data this value shall be calculated as a configurable mathematical function of any of the data fields for each trade secret record using common mathematical and logical expressions.

The value of this field shall be from 1 to a configurable maximum, and each confidentiality level value shall have a configurable text meaning. The configurable maximum shall range from 2 to 5. The default number of confidentiality levels shall be three. The default values for the names of the three confidentiality levels shall be:

- Confidential.
- Top Secret.
- Top Top Secret.

5.4.39 Additional Fields

It shall be possible to define additional fields of trade secret data.

6 Other Data

Other data supported by the system shall include:

- Company data.
- Employee data.
- Configuration data.

6.1 Company Data

Company data shall be able to be entered and viewed only from within the **Administrative Access By Attorneys And Their Assistants** access method.

The following types of company data shall be supported by the system:

6.1.1 Organization Data

Trade Secret Examiner shall support a list of company organizations for use in specifying and cross checking the **Originating Organization For The Trade Secret** field. The system shall support a hierarchical definition of the company organizations to a maximum of five levels, corresponding to the five sub-fields of the **Originating Organization For The Trade Secret** field. The system shall be able to insert a new level above, below, or between existing levels in moving from fewer levels to five levels. The company organizations list shall be composed of organization records that contain the following data for each company organization (group, division, department, etc.):

- Organization Code – the internal company code for the organization. Examples are R&D, Mktg, 4530.
- Organization Name – the internal company name for the organization. Examples are Research & Development Division, Corporate Marketing Department, Software Quality Assurance Group.
- Organization Contact Information – the name, email address, company location, and phone number of the administrator (supervisor, manager, director, etc.) of the organization.
- Reports-To Organization – the internal company code for the organization to which this organization reports.
- Reporting Organizations – the internal company code for the organizations that report to this organization.
- Additional Fields – additional fields shall be configurable by the user.

The system shall be able to display the organization data in outline form and in organization tree form, with one organization fanout per page. The organization tree form of the display shall provide a mouse-driven traversal mechanism.

6.1.2 Location Data

Trade Secret Examiner shall support a list of company locations for use in specifying and cross checking the **Locati n Wh r Th Trad S cr t Was Created, Locations Where The Trade Secret Is Stored,** and **Locations Where The Trade Secret Is Used** fields. The company locations list shall be composed of location records that contain the following data for each company location:

- Location Code – the internal company code for the facility. Examples are HQ, R&D, Chicago, Ireland.
- Location Name – the internal company name for the facility. Examples are Headquarters, Naperville Research & Development Center, Chicago Distribution Center, European Sales Office.
- Location Address – the postal address of the facility.
- Legal Contact Information – the name, email address, and phone number of the legal contact for this facility.
- Security Contact Information – the name, email address, and phone number of the security contact for this facility.
- Security Measures – the selection of security measures in place at this facility.
- Security Threats – the selection of security threats to trade secrets at this facility.
- Additional Fields – additional fields shall be configurable by the user.

6.1.3 Position Data

Trade Secret Examiner shall support a list of company positions for use in calculating the **Employee Position Risk** factor. The company positions list shall be composed of position records that contain the following data for each company position:

- Position Code – the internal company code for the position. Examples are TA, MTS, JA, Ltjg.
- Position Name – the internal company name for the position. Examples are Technical Assistant, Member of the Technical Staff, Junior Associate, Lieutenant Junior Grade.
- Salary Grade – a list of the internal company salary grades available for the position. Examples are 5, 13, O-1, E-9.
- Turnover – a field specifying on a 1 to 5 scale the average turnover of employees with the position.
- Access To Trade Secrets – a field specifying on a 1 to 5 scale the average access to trade secrets of employees with the position.

- Exposure To Outsiders – a field specifying on a 1 to 5 scale the average exposure to outsiders of employees with the position.
- Employee Position Risk Factor – a derived value per section 9.1.4.
- Employee Confidentiality Agreement Renewal Period
- Which Employee Confidentiality Agreement To Be Used
- Employee Confidentiality Reminder Renewal Period
- Which Employee Confidentiality Reminder To Be Used
- Additional Fields – additional fields shall be configurable by the user.

6.2 Employee Data

Employee data shall be able to be entered and viewed only from within the **Administrative Access By Attorneys And Their Assistants** access method.

The following types of employee data shall be supported by the system:

- Employee Name
- Employee Payroll or Badge Number
- Employee Social Security Number
- Employee Salary Grade
- Employee Current Position Code
- Employee Position Code History
- Employee Current Organization Code
- Employee Organization Code History
- Employee Current Location Code
- Employee Location Code History
- Employee Email Address
- Employee Risk Factor
- Last Employee Confidentiality Agreement Renewal Date
- Employee Confidentiality Agreement Renewal Period
- Which Employee Confidentiality Agreement To Be Used
- Last Employee Confidentiality Reminder Renewal Date
- Employee Confidentiality Reminder Renewal Period
- Which Employee Confidentiality Reminder To Be Used
- Employee Data Override Position Data Y/N
- Additional Fields

6.3 Configuration Data

6.3.1 Administrativ Configuration Data

Administrative configuration data shall be able to be entered and viewed only from within the **Administrative Access By Attorneys And Their Assistants** access method.

The following types of other administrative configuration data shall be supported by the system:

- Data recording the configuration values of options, features, and methods declared as configurable throughout this specification, unless specifically declared to be **Superuser Configuration Data**.

6.3.2 Superuser Configuration Data

Superuser configuration data shall be able to be viewed from within the **Administrative Access By Attorneys And Their Assistants** access method and the **Superuser Access** access method. Superuser configuration data shall be able to be entered only from within the **Superuser Access** access method.

The following configuration data shall be superuser configuration data.

- The list of network IDs defined to be within the company.
- Enable status of administrative access via the server console.
- Enable status of administrative access via directly connected LAN.
- Enable status of administrative access via known IP address.
- The list of known IP addresses.
- The expiration dates of known IP addresses.
- Enable status of administrative access via known-number dial-back login.
- The list of known telephone numbers.
- The expiration dates of known telephone numbers.
- User names for administrative access.

7 Data Storage

7.1 Overall Strategy

The overall strategy of the data storage of Trade Secret Examiner shall be that of an accounting system. In particular, data shall never be erased or modified. Data can only be added to. These additions may contain new data intended to supercede old data, but the old superceded data shall also be retained.

7.2 Duration

All trade secret data entered into Trade Secret Examiner must be retained indefinitely. The complete history of all data values, when they were entered, and when and how they were changed, must also be retained indefinitely for all changes. The user making the change shall be recorded and retained indefinitely for all changes to the data.

7.3 Historical Versions

It shall be possible, for any specified date, to generate a version of the database corresponding to its status on that date. This database shall be internally marked as an historical version so that it shall not be possible to use this database to replace the current complete database or to represent this database as the current complete database.

7.4 Audit Trails

The system shall be able to generate an audit trail for at least the following subsets of the database: the complete database; any trade secret within the database; and any individual field of any trade secret record within the database. The system shall be able to generate an audit trail using beginning and ending dates, or to generate an audit trail for all dates.

7.5 Independence Of Multiple Databases

Multiple completely independent Trade Secret Examiner databases shall be supported on all system architectures. Opening any database shall cause a complete overwrite or erasure of all caches, paste buffers, variables, and other data, to prevent contamination of one database with another. It shall not be possible to have more than one Trade Secret Examiner database open at the same time.

7.6 Merge Of Multiple Databases

A merge tool shall be provided as part of Trade Secret Examiner to support the combining of databases. Merge shall be performed through the creation of a new database containing all information, while the old databases shall be retained for archive.

When databases are merged, the trade secret application and certificate numbers shall be differentiated through a prepended alphabetic sequence, such as: #1324 becomes #ABC1324. The prepended sequence shall be able to be up to three characters. The prepending sequence for each database's trade secret application and certificate numbers shall be specified or queried prior to merge.

Merged databases shall catenate weighting curve lists, search lists, location lists, organization lists, and other lists to form merged lists. It shall be possible to state which database being merged is the priority database, and its list members shall be listed first in any merged list. Identical list member names in the two

merging databases shall result in a query to provide unique names for one or both.

Merging of databases that are themselves the products of previous merges shall be possible. In this case, the existing prepended sequence shall be used where it exists unless it is not unique. Identical prepending sequences in the two merging databases shall result in a query to provide unique prepending sequences to replace one or both.

It shall be possible to specify a **Source Status Of The Trade Secret** of "In-House" or "Sold" or "Licensed" for all trade secrets merged, and to enter the associated **Purchased From Information** or **Licensed From Information** for all trade secrets merged.

7.7 Split Of Databases

A split tool shall be provided as part of Trade Secret Examiner to support the creation of sub-databases. Split shall be performed through the creation of a new database containing the split-off information, while the old database retains the entire database. It shall be possible to specify a **Licensing Status Of The Trade Secret** of "Sold" or "Licensed" for all trade secrets split off, and to enter the associated **Sold To Information** or **Licensed To Information** for all trade secrets split-off.

8 Searches

8.1 Search Tools

The following search methods shall be provided for administrative access only by Trade Secret Examiner:

8.1.1 Standard Searches

The system shall be able to generate a list of trade secrets, employee, positions, and locations for the following standard searches:

- Fuzzy search for similar keyword lists, to be used in culling duplicates.
- Date range "from" and "to".
- Fuzzy search for "contains <employee name>".
- Exact search for originating organization, to any precision within the five sub-fields.
- Exact search for "contains <keyword>".
- Exact search for status equals "New".
- Exact search for status equals "Pending Data".
- Exact search for status equals "Pending Review".

- Search for weighted priority greater than specified value using specified weighting.

8.1.2 Custom Search Typ s

The system shall be able to generate a list of trade secrets, employee, positions, and locations for custom searches including:

- Specific values of specific fields.
- Regular expressions.
- Logical operators "and", "or", "xor", and "not".
- Parenthetically-imposed hierarchy.
- "Fuzzy" as an operator; i.e., some fields shall be able to be fuzzy searched while others are exact searched.
- Both "equals" and "contains" as operators for text values.
- Date ranges.
- "Greater than" and "less than" as operators for numeric values.

8.1.3 Custom Search Admin istration

Any custom search specified shall be able to be saved in a list of custom searches associated with the user name.

Any custom search specified shall be able to be configured to be a standard search and included in the standard search menu.

It shall be possible to specify a custom search as a form containing fields to be filled-in at search time.

8.2 Search Results

8.2.1 Drilling Down

Drilling down into any trade secret or other report value shall be provided. Drilling down into an shall bring up the corresponding record. Drilling down into the field name of any field of a record shall bring up the audit trail for the field. Drilling down into the field value of any field of a record shall bring up the description of the field value, or, in the case of organization, location, or position information, bring up the organization, location, or position record. Drilling down into the name of any **Additional Files Required To Document The Trade Secret,** additional files required to document the source status, additional files required to document the licensing status, executed employee confidentiality agreements, or employee confidentiality reminder proofs-of-receipt shall bring up the file for view using an appropriate helper application.

8.2.2 Displaying Lists

The system shall be able to display any list of trade secrets or other records with any of the fields or weightings arranged into any of the columns, such as is possible in Netscape Communicator and Microsoft Windows Explorer. It shall be possible to select a sub-list through drag of the cursor over any list.

8.2.3 Sorting Lists

The system shall be able to sort any list or sub-list of trade secrets or other records in increasing or decreasing order on any field or weighting. Further, it shall be possible to specify secondary and tertiary sorting criteria, and independently specify increasing or decreasing order for each of these.

8.2.4 Printing Lists

The system shall be able to print any list or sub-list generated using the default printer. It shall also be possible to generate a print file for any list or sub-list using .pdf format.

9 Analysis And Reports

9.1 Factor Analysis

The following standard factor analyses shall be provided by Trade Secret Examiner:

9.1.1 Defendability Factors

It shall be possible to specify multiple defendability factors to be calculated from the values for the six factors. The calculation of the defendability factors shall be specified as a mathematical function of the values of the six factors using common mathematical expressions. The system shall be able to save multiple defendability factor functions, and to save multiple defendability factor calculation results for any selection of trade secrets.

9.1.2 Net Present Value Factor

The system shall be able to calculate a net present value factor for each trade secret. The calculation shall consist of sorting all trade secrets in the system into five quintile groups based on the net present value of each trade secret, and providing a net present value factor on a 1 to 5 scale for the trade secrets in each of these quintile groups.

9.1.3 Employee Exposure Factors

The system shall be able to calculate one or more employee exposure factors for each employee. The calculation shall consist of first calculating the employee exposure report for each employee in the system, saving the total number of trade secrets, the net present value of the trade secrets, and the average

defendability of the trade secrets to which the employee was exposed. Employees will be sorted into five quintile groups for each of these exposures, and provided an employee exposure factor on a 1 to 5 scale for the exposures in each of these quintile groups.

9.1.4 Employee Position Risk Factors

The system shall be able to calculate an employee position risk factor for each employee position. This value shall be derived from the risk data associated with each employee position in the employee position record. The list of risks and their weights in calculating this factor shall be configurable. This value shall be configurable as a mathematical function of the weightings of the risk using common mathematical expressions.

9.1.5 Employee Risk Factors

The system shall be able to calculate an employee risk factor for each employee. This value shall be derived from the employee position risk factor and one or more employee exposure factors. This value shall be configurable as a mathematical function of the employee position risk factor and one or more employee exposure factors using common mathematical expressions.

9.2 Standard Reports

The following standard reports shall be provided by Trade Secret Examiner:

9.2.1 Outlier Analysis

The system shall be able to perform an outlier analysis for any list or sub-list of trade secrets generated by the system. This analysis shall look for values of given fields or ratios of given fields which lie outside the main body of trade secrets in the database. It shall be possible to select any field for outlier analysis. It shall be possible to select from a set of ratios for outlier analysis. The list of ratios shall be a configurable option.

The following ratios shall be the default ratios available:

- Any of the six factors/any defendability factor.
- Any defendability factor/net present value factor.
- Security measures factor/security threat factor.

9.2.2 Employee Exposure Report

The system shall be able to generate an employee exposure report documenting an employee's exposure to trade secrets, sorted by the field in which the employee is mentioned. The employee may actually be an employee, contractor, or disclosee of the company. The employee shall be considered to be mentioned if his then-current organization at any time during his employment or association with the company spans the extent to which the trade secret was known within that organization. The employee shall be considered to be mentioned if his then-

current location at any time during his employment or association with the company spans the extent to which the trade secret was known within that location.

In addition to a list of the trade secrets to which the employee has been exposed, the employee's exposure to trade secrets shall be characterized in the following ways:

- Total number of trade secrets to which the employee was exposed.
- Total number of each type of trade secret to which the employee was exposed.
- Total net present value of the trade secrets to which the employee was exposed.
- Average defendability factor of the trade secrets to which the employee was exposed.

9.2.3 Review Schedule Report

The system shall be able to generate a review schedule report documenting the review schedule of any list or sub-list of trade secrets generated by the system for legal review, business review, or both, in several modes: within a range of future dates; overdue for review; and due for review within a specified time.

9.2.4 Review Report

The system shall be able to generate review reports containing all data required to review any list or sub-list of trade secrets generated by the system. One review report shall be generated for each trade secret selected. The information contained in the review report shall be configurable for legal review, business review, or both.

9.2.5 Trade Secret Valuation Report

The system shall be able to generate a trade secret valuation report documenting the current value of any list or sub-list of trade secrets generated by the system. In addition, The system shall be able to generate a report documenting the net present value of any list of trade secrets generated by the system as a function of time for any range of dates.

9.3 Custom Reports

It shall be possible to specify custom reports.

10 Employee Confidentiality Management Tools

10.1 Employee Confidentiality Agreements

The Trade Secret Examiner shall provide the following tools for the management of employee confidentiality agreements.

10.1.1 Employ Confidentiality Agreement R n wal Period

The system shall maintain in the position record for each position a value specifying the employee confidentiality agreement renewal period. The system shall also maintain in the employee record for each employee a value specifying the employee confidentiality agreement renewal period, and whether this value overrides the position value in the position record. The system shall be able to specify this period for all employee records returned by a search of the employee records by position, salary grade, company location, company organization, and other values in the employee record. The system shall also be able to specify this period by employee position and propagate this value to the employee records for all employees.

The system shall be able to search all employee records to find employee records for which the employee confidentiality agreement period has lapsed, or will lapse within a specified time period.

10.1.2 Which Employee Confidentiality Agreement To Be Used

The system shall maintain in the position record for each position a value specifying which employee confidentiality agreement is to be used. The system shall also maintain in the employee record for each employee a value specifying which employee confidentiality agreement is to be used, and whether this value overrides the position value in the position record. The system shall be able to specify which employee confidentiality agreement is to be used for all employee records returned by a search of the employee records by position, salary grade, company location, company organization, and other values in the employee record. The system shall be able to specify which employee confidentiality agreement is to be used by employee position and propagate this value to the employee records for all employees.

The system shall be able to print employee confidentiality agreements for all employee records returned by the search of Section 10.1.1.

10.1.3 Archival Storage Of Executed Employee Confidentiality Agreements

The system shall maintain a scanned image of every executed employee confidentiality agreement, keyed to the employee record. The system shall be able to print out all executed employee confidentiality agreements for any list or sub-list of employee records generated by the system.

10.2 Employee Confidentiality Reminders

The Trade Secret Examiner shall provide the following tools for the management of employee confidentiality reminders.

10.2.1 Employee Confidentiality Reminder Renewal P riod

The system shall maintain in the position record for each position a value specifying the employee confidentiality reminder renewal period. The system shall also maintain in the employee record for each employee a value specifying

the employee confidentiality reminder renewal period, and whether this value overrides the position value in the position record. The system shall be able to specify this period for all employee records returned by a search of the employee records by position, salary grade, company location, company organization, and other values in the employee record. The system shall be able to specify this period by employee position and propagate this value to the employee records for all employees.

The system shall be able to search all employee records to find employee records for which the employee confidentiality reminder period has lapsed, or will lapse within a specified time period.

10.2.2 Which Employee Confidentiality Reminder To Be Used

The system shall maintain in the position record for each position a value specifying which employee confidentiality reminder is to be used. The system shall also maintain in the employee record for each employee a value specifying which employee confidentiality reminder is to be used, and whether this value overrides the position value in the position record. The system shall be able to specify which employee confidentiality reminder is to be used for all employee records returned by a search of the employee records by position, salary grade, company location, company organization, and other values in the employee record. The system shall be able to specify which employee confidentiality reminder is to be used by employee position and propagate this value to the employee records for all employees.

The system shall be able to print employee confidentiality reminders for all employee records returned by the search of Section 10.2.1. The system shall be able to email employee confidentiality reminders for all employee records returned by the search of Section 10.2.1.

10.2.3 Archival Storage Of Proof-Of-Receipt Of Employee Confidentiality Reminders

The system shall maintain a proof-of-receipt for every sent employee confidentiality reminder, keyed to the employee record. The system shall be able to print out all proofs-of-receipt for every sent employee confidentiality reminders for any list or sub-list of employee records generated by the system.

11 Security Management Tools

11.1 Threats/Measures Correlation Matrix

The Trade Secret Examiner shall relate security threats from a list of possible security threats to countering security measures from a list of possible security measures. An acceptable method to meet this requirement is through the use of a correlation matrix, in which the columns are possible security threats and the rows are possible security measures. Entering a value in any position of the matrix indicates that the security measure of that row helps to counter the

security measure of that column. A value from 1 to 5 can be specified, indicating to what extent the security measure counters the security threat. The sum of values for all security measures in place in response to a given threat must total five or more for that threat to be considered countered by the security measures.

11.2 Correlation Of Threats And Measures

The Trade Secret Examiner shall be able to perform a correlation analysis of the security measures in place to counter the security threats to trade secrets for any list or sub-list of company locations or trade secrets generated by the system. For each security threat identified for each location or trade secret in the list, the system shall add up the correlation matrix values for each security measure in place for that location or trade secret. The system shall prepare a report listing each location or trade secret for which the sum of the correlation matrix values for any security threat to trade secrets for that company location or trade secret is less than five.

11.3 Counter-Threat Status

The Trade Secret Examiner shall be able to associate a counter-threat status with each security threat to each company location and trade secret in the system. For 10 threats, 15 locations, and 1000 trade secrets, 150000 counter-threat status values are required to meet this requirement. The counter-threat status will initially be given a value of "Uncountered". A value of "Countered" will be given to any threat found to be countered with a value of five or more by the correlation analysis of Section 11.2. A value of "Partially Countered" will be given to any threat found to be countered with a value of greater than zero and less than five by the correlation analysis of Section 11.2.

It shall be possible to modify this value for any threat to any company location or trade secret, for any threat to all company locations or trade secrets in a list or sub-list, or for all threats to all company locations or trade secrets in a list or sub-list. However, it shall not be possible to manually assign a value of "Countered" or "Partially Countered" to any threat. The default values available for the counter-threat status shall be:

- Uncountered – no security measure is in place to counter this threat.
- Partially Countered – some security measures are in place to counter this threat.
- Countered – adequate security measures are in place to counter this threat.
- Planned – adequate security measures are planned to counter this threat.
- Acceptable – The risk posed by the security threats to this company location or trade secret have been reviewed and deemed acceptable.

12 Trad Secret Verification Tools

The Trade Secret Examiner shall provide tools to aid in the later verification of the existence of trade secret data at an earlier time. The Trade Secret Examiner shall provide the following tools to aid in trade secret verification.

12.1 Trade Secret Database Segmentation

It shall be possible to configure the system to support multiple segments of the trade secret database. These segments shall be specified through the use of configuration information that specifies, for each segment of the data, which fields of the trade secret records lie within that segment. It shall be possible for a field to lie within more than one database segment. The following segments shall be the default:

- Total – contains all fields of the trade secret record.
- Technical – contains the **Name Of The Trade Secret, Keywords Associated With The Trade Secret, Description Of The Trade Secret, Patentability Of The Trade Secret, Additional Files Required To Document The Trade Secret, Trade Secret Type**.
- Financial – contains the **Date The Trade Secret Was Created, Patentability Of The Trade Secret, Estimated Life Expectancy Of The Trade Secret, Source Status Of The Trade Secret, Licensing Status Of The Trade Secret, Trade Secret Value, Trade Secret Depreciation Method and Schedule, Net Present Value**.
- Legal – contains the **Date The Trade Secret Was Created, Date The Trade Secret Application Was Entered, Trade Secret Applicant, Inside Knowledge Factor, Outside Knowledge Factor, Investment Factor, Economic Benefit Factor, Reproducibility Factor, Security Measures Factor, Patentability Of The Trade Secret, Estimated Life Expectancy Of The Trade Secret, Validity Status Of The Trade Secret, Source Status Of The Trade Secret, Licensing Status Of The Trade Secret, Legal Reviewer Level Of The Trade Secret, Last Legal Review Date, Last Legal Reviewer, Legal Reviewer Comments, Legal Review Schedule**.
- Business – contains the **Business Reviewer Level Of The Trade Secret, Last Business Review Date, Last Business Reviewer, Business Reviewer Comments, Business Review Schedule, Trade Secret Type**.
- Security – contains the **Security Measures, Security Threat Factor Of The Trade Secret, Confidentiality Levels**.

12.2 Trade Secret Database Segment Hashing

The system shall be able to generate a hash of any database segment of any list or sub-list of trade secrets generated by the system. The hash codes shall be calculated using deterministic secure one-way hash codes. The size of the hash

codes and the calculation method shall be selected for the characteristics of uniformity of distribution and limited probability of duplication.

It shall always be possible to generate the same hash code at a later date, whether or not the data has been updated in the intervening period.

12.3 Other Data Hashing

The system shall be able to generate hashes of the other data in the system, for later verification of the existence, format, and contents of the other data. Separate hashes shall be generated for Company Data, Employee Data, Configuration Data, Employee Confidentiality Data, including executed employee confidentiality agreements and proofs-of-receipt of employee confidentiality reminders, and Security Management Data.

It shall be possible to generate hashes for any selection of data in the system.

It shall always be possible to generate the same hash code at a later date, whether or not the data has been updated in the intervening period.

13 Interfaces To Other Systems

13.1 Interface To Trade Secret Directory

The system shall include an interface to the Trade Secret Office, Inc. Trade Secret Directory server. All messages transmitted and received over this interface shall be archived by the system indefinitely. This interface shall provide the following services:

13.1.1 Certificate Request

Trade secret registration will be accomplished by sending a trade secret certificate request to the Trade Secret Directory. This request may be sent by Internet email message, floppy disk, or CD-ROM. The trade secret certificate request shall include the following data:

- The serial number of this copy of Trade Secret Examiner
- Application Number for the trade secret
- Application Hash Codes for the trade secret
- Certificate or registration number for the immediately previous trade secret certificate or registration response received from the Trade Secret Directory.
- Certificate or registration code for the immediately previous trade secret certificate or registration response received from the Trade Secret Directory.

13.1.2 Certificate R sponse

A trade secret certificate request may result in the receipt of a trade secret certificate from the Trade Secret Directory. This certificate may be received by

Internet email message, floppy disk, or CD-ROM. The certificate shall include the following data:

- The serial number of this copy of Trade Secret Examiner
- Application Number for the trade secret
- Application Hash Codes for the trade secret
- Certificate Number for the trade secret
- Certificate Hash Code for the trade secret

13.1.3 Certificate Revision Request

Trade secret revision registration will be accomplished by sending a trade secret certificate revision request to the Trade Secret Directory. This request may be sent by Internet email message, floppy disk, or CD-ROM. The trade secret certificate revision request shall include the following data:

- The serial number of this copy of Trade Secret Examiner
- Application Number for the revised trade secret
- Application Hash Codes for the revised trade secret
- Certificate Number originally received for the trade secret
- Certificate Hash Code originally received for the trade secret
- Certificate or registration number for the immediately previous trade secret certificate or registration response received from the Trade Secret Directory.
- Certificate or registration code for the immediately previous trade secret certificate or registration response received from the Trade Secret Directory.

13.1.4 Certificate Revision Response

A trade secret certificate request may result in the receipt of a trade secret certificate from the Trade Secret Directory. This certificate may be received by Internet email message, floppy disk, or CD-ROM. The certificate shall include the following data:

- The serial number of this copy of Trade Secret Examiner
- Application Number for the revised trade secret
- Application Hash Codes for the revised trade secret
- Certificate Number for the trade secret
- Certificate Hash Code for the trade secret

13.1.5 Registration R quest

Registration of other data in the system will be accomplished by sending a registration request to the Trade Secret Directory. This request may be sent by

Internet email message, floppy disk, or CD-ROM. The registration request shall include the following data:

- The serial number of this copy of Trade Secret Examiner
- Hash code for the data to be registered
- Certificate or registration number for the immediately previous trade secret certificate or registration response received from the Trade Secret Directory.
- Certificate or registration code for the immediately previous trade secret certificate or registration response received from the Trade Secret Directory.

13.1.6 Registration Response

A registration request may result in the receipt of a registration response from the Trade Secret Directory. This certificate may be received by Internet email message, floppy disk, or CD-ROM. The certificate shall include the following data:

- The serial number of this copy of Trade Secret Examiner
- Hash code for the data to be registered
- Registration number for the data to be registered
- Registration code for the data to be registered

13.1.7 Verification Request

A trade secret certificate request may result in the receipt of a verification request from the Trade Secret Directory. Verification requests may also be received at other times. Verification requests may be received by Internet email message, floppy disk, or CD-ROM. The verification request shall include the following data:

- The serial number of this copy of Trade Secret Examiner
- Certificate or registration number for the first trade secret or registration to be verified
- Certificate or registration code for the first trade secret or registration to be verified
- Certificate or registration number for the second trade secret or registration to be verified
- Certificate or registration code for the second trade secret or registration to be verified
- and so on.

13.1.8 Verification Response

A verification request from the Trade Secret Directory shall be answered with a verification response. The verification response will indicate for each trade secret or registration whether or not the certificate number and certificate hash

code matched those contained in the system's database or not. Verification responses may be sent by Internet email message, floppy disk, or CD-ROM. The verification response shall include the following data:

- The serial number of this copy of Trade Secret Examiner
- Certificate or registration number for the first trade secret or registration to be verified
- Certificate or registration code for the first trade secret or registration to be verified
- Indication of whether the first trade secret or registration verified or not
- Certificate or registration number for the second trade secret or registration to be verified
- Certificate or registration code for the second trade secret or registration to be verified
- Indication of whether the second trade secret or registration verified or not
- and so on.

13.2 Interface To SAP

The system shall include an interface to SAP sufficient to download employee data from the SAP system.

13.3 Interface To PeopleSoft

The system shall include an interface to PeopleSoft sufficient to download employee data from the PeopleSoft system.

14 Additional Tools

14.1 Scanning Of Documents

The system shall be able to scan documents into Trade Secret Examiner for the purpose of generating **Additional Files Required To Document The Trade Secret,** additional files required to document the source status, additional files required to document the licensing status, executed employee confidentiality agreements, and employee confidentiality reminder proofs-of-receipt.

14.2 Helper Applications

It shall be possible to configure Trade Secret Examiner to call helper applications to aid in the viewing of **Additional Files Required To Document The Trade Secret,** additional files required to document the source status, additional files required to document the licensing status, executed employee confidentiality agreements, and employee confidentiality reminder proofs-of-receipt.

14.3 Trade Secret Law Advisories

The system shall contain a help function for access to advice on trade secret law. This information shall also be available via an index and with search tools. This information shall also be available via context-sensitive help on the right mouse button.

At appropriate points in the use of the system, the system shall point out features of the law that may apply directly to the user's current activities. This feature shall be configurable to provide: no advisory; indication of an appropriate advisory in the frame of the current window; advisory displayed in the frame of the current window.

This information shall be able to be updated via a network connection to the web page of The Trade Secret Office, Inc.

15 Appendix A: Feature Package Contents

The features available in each of the various system architectures, and the features to be included in each release of the system, are to be defined.

16 Appendix B: Trade Secr t Types

16.1 Structure

The structure of the trade secret type designation shall be a three-level hierarchy, corresponding to the department within the company, the general form of the trade secret, and then the specific type of secret. The default configuration shall be that one alphanumeric character shall define each level, such as ED7 or ASB. Departments and forms need not be unique for a character: Accounting and Administrative can share the "A" designation at the first level, for example. It shall also be possible to define a two-letter code for each level to achieve uniqueness, such as Ad for Administration and Ac for Accounting, or top specify an unused letter for one of the non-unique values, such as C for Accounting.

The values for the first two levels shall form a matrix with cells for each general form of trade secret within each department. Each cell shall be able to be configured with specific types of trade secret, independently of the other cells. These specific types shall be numbered or lettered in sequence. If numbered, it shall be possible to specify two digits for each specific type of trade secret.

If there is more than one department or general form of trade secret in a cell, such as cell AL holding both Accounting Lists and Administrative Lists, the range of numbers or letters shall be divided between them. Accounting would range from 1-50 and Administrative from 51 to 100 in the example.

It shall be possible to add entries to each level within the hierarchy. The default entries in the hierarchy shall be as given in Section 11.2. It shall be possible to configure entries in the hierarchy as unused, rather than erasing them from the system, to allow building of new entries in advance of use or to reserve entries for future use.

16.2 Default Entries

16.2.1 Departments

The following departments shall be the default values for the first level of the hierarchy. The first letter of the department shall be the code. It shall be possible to use other letters or additional letters in order to achieve unique department designators.

- Accounting
- Administrative
- Business Development
- Communications
- Customer Care
- Development
- Engineering
- Finance
- General & Administrative

- Human Resources
- Information Technology
- Manufacturing
- Marketing
- Purchasing
- Physical Plant
- Quality Assurance
- Research
- Sales
- Testing
- Technology
- Transportation

16.2.2 General Form Of The Trade Secret

The following general forms of the trade secret shall be the default values for the second level of the hierarchy. The first letter of the general form shall be the code. It shall be possible to use other letters or additional letters in order to achieve unique general form designators.

- Budgets
- Contracts
- Costs
- Diagrams
- Drawings
- Equipment
- Forecasts
- Know-How
- Lists
- Meeting Minutes
- Methods
- Negative Know-How
- Pert Charts
- Plans
- Processes
- Programs
- Prototypes
- Results
- Schedules
- Spreadsheets
- Techniques

16.2.3 Specific Type Of The Trade Secret

The default values for the specific type of trade secret in each cell are to be defined.